AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original ☐

CLERK'S OFFICE
A TRUE COPY
Feb 07, 2023
s/ D. Olszewski
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wiscons

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information about the location of the cellular telephone assigned IP Address: 2607:fb90:d30b:327c:ac39:9491:4e86:9aac, which was utilized multiple times, as listed in Attachment A, between December 7, 2022, and February 1, 2023 (the "Target Cell Phone"), whose service provider is T-Mobile ("Service Provider")

Case No. 23 MJ 11

Matter No.: 2022R00305

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin
(identify the person or describe the property to be searched and give its location):

Please see Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

Please see Attachment B.

YOU ARE COMMANDED to execute this warrant on or before February 7, 2023 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable William E. Duffin.
(United States Magistrate Judge)

☑ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☑ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 02/07/2023 1:41 pm

William E. Duffin
Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S. Magistrate
Printed name and title

Return

Case No.: 23 MJ 11	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Print Save As... Reset

ATTACHMENT A

Property to Be Searched

Records and information associated with the cellular device assigned IP Address 2607:fb90:d30b:327c:ac39:9491:4e86:9aac, utilized at the following dates and times:

- Time 2023-02-01 23:11:00 UTC
- Time 2023-02-01 22:54:35 UTC
- Time 2023-02-01 22:22:09 UTC
- Time 2023-02-01 21:52:48 UTC
- Time 2023-02-01 21:14:41 UTC
- Time 2023-02-01 20:54:27 UTC
- Time 2023-02-01 20:38:41 UTC
- Time 2023-02-01 20:05:09 UTC
- Time 2023-02-01 19:36:27 UTC

(Referred to herein and in Attachment B as "the Target Cell Phone"), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan, Parsippany, NJ 07054

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of 01/02/2023 to the date of this warrant's execution:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received) as well as per-call measurement data (also known as "real-time tool" or "RTT")].

b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as "real-time tool" or "RTT").

The Court has also issued an order pursuant to 18 U.S.C. § 3123, for such information associated with the Target Cell Phone.

c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. "Information about the location of the Target Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information about the location of the cellular telephone assigned IP Address: 2607:fb90:d30b:327c:ac39:9491:4e86:9aac, which was utilized multiple times, as listed in Attachment A, between December 7, 2022, and February 1, 2023 (the "Target Cell Phone"), whose service provider is T-Mobile ("Service Provider")

Case No. 23 MJ 11

Matter No.: 2022R00305

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

Please see Attachment A.

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §751	ESCAPE FROM CUSTODY RESULTING FROM CONVICTION

The application is based on these facts:

Please see attached Affidavit.

- ☑ Continued on the attached sheet.
- ☑ Delayed notice of 30 days *(give exact ending date if more than 30 days: _____)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

DAKOTAH URBAN Digitally signed by DAKOTAH URBAN Date: 2023.02.06 12:35:02 -06'00'

Applicant's signature

Dakotah Urban, Deputy U.S. Marshal

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 2/7/2023

William E. Duffin

Judge's signature

City and state: Milwaukee, WI

Honorable William E. Duffin, U.S Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Deputy United States Marshal Dakotah Urban, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant under Federal Rule of Criminal Procedure 41 and 18 U.S.C. §§ 2703(c)(1)(A), for information about the location of the cellular telephone assigned IP Address: **2607:fb90:d30b:327c:ac39:9491:4e86:9aac**, which was utilized multiple times, as listed in Attachment A, between December 7, 2022, and February 1, 2023 (the "Target Cell Phone"), whose service provider is T-Mobile ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan, Parsippany, NJ 07054. The Target Cell Phone is described herein and in Attachment A, and the location information to be seized is described herein and in Attachment B.

2. Because this warrant application seeks the prospective collection of information, including cell-site location information, that may fall within the statutory definitions of information collected by a "pen register" and/or "trap and trace device," *see* 18 U.S.C. § 3127(3) & (4), I also make this affidavit in support of an application by the United States of America for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the Target Cell Phone.

3. I, Dakotah Urban, am a Deputy United States Marshal (DUSM) and have been employed by the United States Marshal Service (USMS) for approximately 4-years. One of my primary duties as a DUSM is to investigate, locate, and arrest state and federal Fugitives. I

obtained my criminal investigation training certification at the Federal Law Enforcement Training Center (FLETC) located in Glynco, GA. During my training at FLETC, I completed the federal Criminal Investigator Training Program (CITP) along with the Basic Deputy United States Marshal (BDUSM) training.

4. I am regularly assigned cases related to fugitive apprehension and have been involved in numerous prior fugitive cases. Many of these investigations were aided by procurement of records related to electronic communications and subsequent analysis of those records. In most of those cases, the records provided critical investigative leads and corroborative evidence and information. I have had previous experiences using electronic location data in order to locate and apprehend fugitives from justice. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), in that I am empowered by law to conduct investigations.

5. The facts in this affidavit come from my training, experience and information provided to me by other Law Enforcement Officers and my review of documents and information obtained from other agents. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, there is probable cause to believe that Wayne A. Scott Jr. has violated 18 U.S.C. § 751(a) (Escape from Custody).

7. There is also probable cause to believe that the information described in Attachment B will assist law enforcement in arresting SCOTT, who is a "person to be arrested" within the meaning of Federal Rule of Criminal Procedure 41(c)(4).

JURISDICTION

8. The court has jurisdiction to issue the proposed warrant because it is a "court of competent jurisdiction" as defined 18 U.S.C. § 2711. Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated, *see* 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

9. On November 22, 2022, a criminal complaint was submitted charging Wayne A. Scott Jr. with 18 U.S.C. § 751(a) (Escape from Custody). An arrest warrant was issued and assigned Case No. 22-1850M(NJ).

10. Since the issuance of this arrest warrant, the United States Marshal Service Fugitive Task Force has made attempts to arrest Mr. Scott at his known address and has conducted surveillance at other known locations but have been unsuccessful in locating him. Mr. Scott has also been publicly profiled on Fox6 News, Milwaukee's Most Wanted as an active fugitive but has still failed to surrender to authorities.

11. On November 30, 2022, the USMS, through an open search, located the Facebook account "Waun Lewis" with url: https://www.facebook.com/profile.php?id=100073404194027 This account depicted a profile picture of Wayne A. Scott Jr. and other facial photos of the subject, which were compared to booking photos and Department of Transportation (DOT) photos and were determined to be the same person.

12. On that same day, November 30, 2022, that Facebook profile, "Waun Lewis" posted a 24-hour story to his timeline. The story was discovered by the USMS at 1:02 pm and according to Facebook, was posted by "Waun Lewis" approximately 20-hours prior. The

picture posted to the Facebook story portrayed a bottle of Hennessy with the background audio of a song by MarijuanaXO and Slim Dawg Millionaire titled, *Andrew Luck*.

13. On December 7th, 2022, an Order Authorizing the Installation and Use of a Pen Register Trap and Trace was signed by US Magistrate Judge William Duffin. This signed order produced data about the location and usage of the mentioned Facebook account. This order is currently active and valid until Sunday, February 5th, 2023.

14. Results of the on-going pen register trap and trace of Facebook account, https://www.facebook.com/profile.php?id=100073404194027, show that between the dates of December 7, 2022, through February 1, 2023, log-in IP addresses for the account have appeared and verifies that SCOTT has been utilizing his account. Identified IP addresses show that there is consistent usage of a T-Mobile cellular device. The most recent IP Address is shown to be, 2607:fb90:9a01:4e0d:0000:0005:b295:6b01, utilized on 2021-04-25 23:38:12 UTC (the "Target Cell Phone"), whose service provider is T-Mobile ("Service Provider"), a wireless telephone service provider headquartered at 4 Sylvan, Parsippany, NJ 07054.

15. The affiant knows that subjects who are wanted for crimes and are trying to remain "at large" use social media frequently to communicate with family/friends/co-actors. It is common for wanted subjects to set these social media accounts to "Private" or lock the access to them, use alias names, and use accounts of other persons to remain undetected by law enforcement authorities.

TECHNICAL BACKGROUND: DYNAMIC IP ADDRESSES

16. Your affiant utilized the website www.arin.net, the "American Registry of Internet Numbers (ARIN)," to obtain the owner and operator of the IP address mentioned previously: 2607:fb90:d30b:327c:ac39:9491:4e86:9aac, which was utilized multiple times listed

in Attachment A between December 7, 2022, and February 1, 2023. According to ARIN, the listed IP address is owned and operation by T-Mobile. Your affiant has utilized ARIN in the past and knows this website to be reliable.

17. Based on training, experience and information provided to me by other Law Enforcement Officers, I know that T-Mobile is a cellular service provider and does have the ability to connect their cellular service to the internet through Dynamic Internet Protocols. A dynamic Internet Protocol address (dynamic IP address) is a temporary IP address that is assigned to a computing device or node when it's connected to a network. A dynamic IP address is an automatically configured IP address assigned by a Dynamic Host Configuration Protocol (DHCP) server to every new network node.

18. Dynamic IP addresses are generally implemented by Internet service providers and networks that have a large number of connecting clients or end-nodes. Unlike static IP addresses, dynamic IP addresses are not permanent. A dynamic IP is assigned to a node until it's connected to the network; therefore, the same node may have a different IP address every time it reconnects with the network.

19. I know through training, experience and information provided to me by other Law Enforcement Officers that T-Mobile is able to "resolve" associated Dynamic IP addresses. When T-Mobile "resolves" those IP addresses, they are able to identify the associated user and the specific cellular phone associated with that user. In other words, when T-Mobile is provided with a particular associated IP address and time stamp (like the IP address and time stamp described here), T-Mobile is able to (i) determine the particular cellular phone that utilized that IP address; and (ii) collect cell-site location data associated with that same particular cellular phone, in the manner described below.

TECHNICAL BACKGROUND: CELL SITE LOCATION DATA

20. In my training, experience and information provided to me by other Law Enforcement Officers, I have learned that the Service Provider is a company that provides cellular communications service to the general public. I also know that providers of cellular communications service have technical capabilities that allow them to collect and generate information about the locations of the cellular devices to which they provide service, including cell-site data, also known as "tower/face information" or "cell tower/sector records." Cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular device and, in some cases, the "sector" (i.e., faces of the towers) to which the device connected. These towers are often a half- mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data provides an approximate general location of the cellular device.

21. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that the Service Provider can collect cell-site data on a prospective basis about the Target Cell Phone. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that for each communication a cellular device makes, its wireless service provider can typically determine: (1) the date and time of the communication; (2) the telephone numbers involved, if any; (3) the cell tower to which the customer connected at the beginning of the communication; (4) the cell tower to which the customer was connected at the end of the communication; and (5) the duration of the communication. I also know that wireless providers such as the Service Provider typically collect and retain cell-site data pertaining to cellular devices to which they provide service in their

normal course of business in order to use this information for various business-related purposes.

22. I know that some providers of cellular telephone service have technical capabilities that allow them to collect and generate E-911 Phase II data, also known as GPS data or latitude-longitude data. E-911 Phase II data provides relatively precise location information about the cellular telephone itself, either via GPS tracking technology built into the phone or by triangulating on the device's signal using data from several of the provider's cell towers. As discussed above, cell-site data identifies the "cell towers" (i.e., antenna towers covering specific geographic areas) that received a radio signal from the cellular telephone and, in some cases, the "sector" (i.e., faces of the towers) to which the telephone connected. These towers are often a half-mile or more apart, even in urban areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to a wireless device does not necessarily serve every call made to or from that device. Accordingly, cell-site data is typically less precise that E-911 Phase II data. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that the Service Provider can collect E-911 Phase II data about the location of the Target Cell Phone, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available.

23. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know each cellular device has one or more unique identifiers embedded inside it. Depending on the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), a Mobile

Subscriber Integrated Services Digital Network Number ("MSISDN"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Equipment Identity ("IMEI"). The unique identifiers – as transmitted from a cellular device to a cellular antenna or tower – can be recorded by pen-trap devices and indicate the identity of the cellular device making the communication without revealing the communication's content.

24. Based on my training, experience and information provided to me by other Law Enforcement Officers, I know that wireless providers such as the Service Provider typically collect and retain information about their subscribers in their normal course of business. This information can include basic personal information about the subscriber, such as name and address, and the method(s) of payment (such as credit card account number) provided by the subscriber to pay for wireless communication service. I also know that wireless providers such as the Service Provider typically collect and retain information about their subscribers' use of the wireless service, such as records about calls or other communications sent or received by a particular device and other transactional records, in their normal course of business. In my training, experience and information provided to me by other Law Enforcement Officers, this information may constitute evidence of the crimes under investigation because the information can be used to identify the Target Cell Phone's user or users and may assist in the identification of co-conspirators and/or victims.

25. Based on the foregoing, I request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

26. I further request that the Court direct the Service Provider to disclose to the government any information described in Section I of Attachment B that is within its possession,

custody, or control.

27. I also request that the Court direct the Service Provider to furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the information described in Attachment B unobtrusively and with a minimum of interference with the Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall reasonably compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

28. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 30 days after the collection authorized by the warrant has been completed. There is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the subscriber or user of the Target Cell Phone would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). As further specified in Attachment B, which is incorporated into the warrant, the proposed search warrant does not authorize the seizure of any tangible property. *See* 18 U.S.C. § 3103a(b)(2). Moreover, to the extent that the warrant authorizes the seizure of any wire or electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or electronic information, there is reasonable necessity for the seizure for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

29. Because the warrant will be served on the Service Provider, who will then

compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. I further request that the Court authorize execution of the warrant at any time of day or night, owing to the potential need to locate the Target Cell Phone outside of daytime hours.

ATTACHMENT A

Property to Be Searched

Records and information associated with the cellular device assigned IP Address 2607:fb90:d30b:327c:ac39:9491:4e86:9aac, utilized at the following dates and times:

- Time 2023-02-01 23:11:00 UTC
- Time 2023-02-01 22:54:35 UTC
- Time 2023-02-01 22:22:09 UTC
- Time 2023-02-01 21:52:48 UTC
- Time 2023-02-01 21:14:41 UTC
- Time 2023-02-01 20:54:27 UTC
- Time 2023-02-01 20:38:41 UTC
- Time 2023-02-01 20:05:09 UTC
- Time 2023-02-01 19:36:27 UTC

(Referred to herein and in Attachment B as "the Target Cell Phone"), that is in the custody or control of T-Mobile (referred to herein and in Attachment B as the "Service Provider"), a wireless communications service provider that is headquartered at 4 Sylvan, Parsippany, NJ 07054

ATTACHMENT B

Particular Things to be Seized

I. Information to be Disclosed by the Provider

To the extent that the information described in Attachment A is within the possession, custody, or control of the Service Provider, including any information that has been deleted but is still available to the Service Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Service Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A:

a. The following subscriber and historical information about the customers or subscribers associated with the Target Cell Phone for the time period of 01/02/2023 to the date of this warrant's execution:

i. Names (including subscriber names, user names, and screen names);

ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);

iii. Local and long distance telephone connection records;

iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;

v. Length of service (including start date) and types of service utilized;

vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifier ("MEID"); Mobile Identification Number ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"); International Mobile Subscriber Identity Identifiers ("IMSI"), or International Mobile Equipment Identities ("IMEI");

vii. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and

viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.

ix. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Target Cell Phone, including:

(A) the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and

(ii) information regarding the cell tower and antenna face (also known as "sectors" through which the communications were sent and received) as well as per-call measurement data (also known as "real-time tool" or "RTT")].

b. Information associated with each communication to and from the Target Cell Phone for a period of 30 days from the date of this warrant, including:

i. Any unique identifiers associated with the cellular device, including ESN, MEIN, MSISDN, IMSI, SIM, or MIN;

ii. Source and destination telephone numbers;

iii. Date, time, and duration of communication; and

iv. All data about the cell towers (i.e. antenna towers covering specific geographic areas) and sectors (i.e. faces of the towers) to which the Target Cell Phone will connect at the beginning and end of each communication as well as per-call measurement data (also known as "real-time tool" or "RTT").

The Court has also issued an order pursuant to 18 U.S.C. § 3123, for such information associated with the Target Cell Phone.

c. Information about the location of the Target Cell Phone for a period of 30 days, during all times of day and night. "Information about the location of the Target Phone" includes all available E-911 Phase II data, GPS data, latitude-longitude data, and other precise location information.

i. To the extent that the information described in the previous paragraph (hereinafter, "Location Information") is within the possession, custody, or control of the Service Provider, the Service Provider is required to disclose the Location Information to the government. In addition, the Service Provider must furnish the government all information, facilities, and technical assistance necessary to accomplish the collection of the Location Information unobtrusively and with a minimum of interference with the

Service Provider's services, including by initiating a signal to determine the location of the Target Cell Phone on the Service Provider's network or with such other reference points as may be reasonably available, and at such intervals and times directed by the government. The government shall compensate the Service Provider for reasonable expenses incurred in furnishing such facilities or assistance.

ii. This warrant does not authorize the seizure of any tangible property. In approving this warrant, the Court finds reasonable necessity for the seizure of the Location Information. *See* 18 U.S.C. § 3103a(b)(2).

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. Section 751(a), (Escape from Custody). An arrest warrant (E/WI Case No.22-1850M(NJ)) authorized for nationwide extradition was issued on November 11, 2022, for the arrest of Wayne A. Scott Jr., (M/B, 10/10/1992) including, but not limited to, information pertaining to the following matters:

(a) SCOTT's location(s)

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. Section 751(a), (Escape from Custody). An arrest warrant (E/WI Case No.22-1850M(NJ)) authorized for nationwide extradition was issued on November 11, 2022, for the arrest of Wayne A. Scott Jr., (M/B, 10/10/1992) including, but not limited to, information pertaining to the following matters:

(a) SCOTT's location(s)

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Service Provider in order to locate the things particularly described in this Warrant.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by AT&T, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of AT&T. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of AT&T, and they were made by AT&T as a regular practice; and

b. such records were generated by AT&T electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of AT&T in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by AT&T, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature